UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRUCE YUILLE, an individual consumer, Plaintiff, v. UPHOLD HQ, INC, Defendant.	**CIVIL ACTION NO.:** **COMPLAINT AND JURY DEMAND**

COMPLAINT

Plaintiff Bruce Yuille ("Mr. Yuille"), by and through his undersigned attorneys, makes the following factual allegations applicable to each cause of action pled herein against defendant Uphold HQ, Inc. ("Uphold").

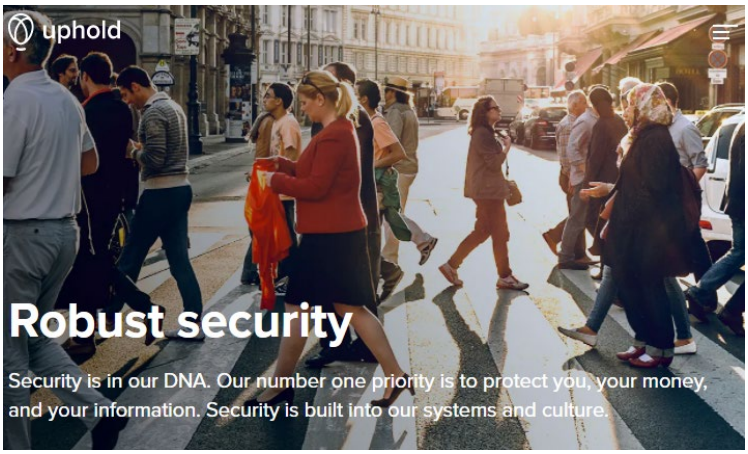
PRELIMINARY STATEMENT

1. Mr. Yuille entrusted approximately 100 Bitcoin ("BTC") to Uphold to safeguard, believing that Uphold would provide robust security for his BTC. Despite Uphold's assurances of robust security, after multiple failed attempts by an unauthorized party to access Mr. Yuille's account over two days, Uphold permitted an unauthorized party to change the email address and password on Mr. Yuille's account and to access Mr. Yuille's account. Even after Mr. Yuille provided immediate notice to Uphold that he was locked out his account, Uphold took no action to stop that unauthorized party from electronically transferring approximately 100 BTC—then valued at nearly $5,000,000—out of Mr. Yuille's Uphold consumer digital asset account (all transfers occurring in the two days *after* Mr. Yuille provided Uphold with notice). As such, Mr. Yuille brings this claim to recover approximately $5,000,000 in actual damages that he suffered as a direct result of Uphold's negligence and other wrongdoing, approximately $15,000,000 in

treble damages for Uphold's violations of the Electronic Funds Transfer Act, 15 U.S.C. § 1693 and Regulation E (the "EFTA") and N.Y. Bus. Law § 349, as well as attorneys' fees, and costs.

2. Uphold is a cryptocurrency exchange and digital money platform with more than 1.7 million customers globally and nearly $6 billion in transactions since its inception. Uphold describes itself as a "multi-asset digital money platform offering financial services to a global market."[1]

3. Uphold holds itself out as a secure cryptocurrency platform and touts as such on its website:



State-of-the art security

Security is in our DNA. We obsess about it. Our top priority is to protect you, your money, and your information. Uphold is a community. We enforce stringent security standards across our platform - and continually educate our customers on the important role they have to play.

4. Uphold's website further represents that "[t]he Uphold Security Operations Centre monitors systems year-round and responds immediately to any detected threat."[2]

[1] *See* Uphold, Resources, available at https://uphold.com/en-us/resources/about (last visited April 18, 2022).
[2] *See* Uphold, Security, available at https://uphold.com/en-us/get-started/security (last visited April 18, 2022).

5. Despite these representations, Uphold failed to respond adequately or reasonably to an open and obvious threat on Mr. Yuille's account after Mr. Yuille notified Uphold that he was locked out of his account, failed to restrict access to Mr. Yuille's account even after receiving notice from Mr. Yuille of obvious security red flags, and failed to implement measures to prevent third parties from obtaining unauthorized access to Mr. Yuille's Uphold account and the assets contained therein.

6. Uphold's failure to restrict access to Mr. Yuille's account and its lack of sufficient safeguards that would prevent unauthorized access to Mr. Yuille's account resulted in unauthorized third parties transferring approximately $5,000,000 of cryptocurrency assets out of Mr. Yuille's account.

7. Both prior to the unauthorized electronic transfers of Mr. Yuille's BTC and after the unauthorized transfers, Uphold failed to comply with its EFTA obligations. Among other things, Uphold failed to: provide the mandated disclosures before the first electronic transfer was made; investigate the erroneous electronic transfers; provisionally credit Mr. Yuille's account for the improperly transferred assets; give Mr. Yuille use of the improperly transferred assets during Uphold's investigation; report the results of its investigation within thirteen (13) days of the error; or correct the erroneous transfers out of Mr. Yuille's account.

8. Mr. Yuille seeks compensatory, statutory, and equitable relief from Uphold as compensation for the loss of cryptocurrency that directly resulted from Uphold permitting unauthorized access to Mr. Yuille's account.

I. PARTIES, JURISDICTION AND VENUE,

9. Mr. Yuille is a 77-year-old individual consumer who lives in Clarkston, Oakland County, Michigan. At all times material hereto, he was Uphold's customer and had a consumer account with Uphold.

10. Uphold has its principal place of business in New York, New York. Uphold is a financial institution that maintains consumer accounts for consumers worldwide to safeguard, transfer, and trade cryptocurrencies and other assets.

11. This Court has original subject matter jurisdiction over this case because Mr. Yuille's claim under the EFTA, 15 U.S.C. § 1693, arises under the laws of the United States. 28 U.S.C. §1331.

12. This Court has original subject matter jurisdiction because the amount in controversy exceeds $75,000 and Mr. Yuille and Uphold are citizens of different states. 28 U.S.C. §1332.

13. The Court has general personal jurisdiction over Uphold, whose principal places of business is in the State of New York.

14. Venue is proper pursuant to 28 U.S.C. § 1391(b)(1) and (2), as Uphold resides in this District and a substantial part of the events or omissions giving rise to the claim occurred in this District.

II. FACTUAL ALLEGATIONS

15. Uphold is a cryptocurrency and asset exchange that allows users to transfer, purchase, trade, hold, and sell cryptocurrencies as well as select equities, precious metals, and

currencies. It holds itself out as "a digital money platform providing consumers worldwide with convenient and secure access to traditional currencies, cryptocurrencies, and other investments."[3]

16. Uphold purports to allow and enable consumers to securely convert and transact in traditional currencies, cryptocurrencies, and precious metals. Specifically, Uphold represents on its website that its "unique 'Anything-to-Anything' trading experience enables customers to trade directly between asset classes with embedded payments" and that its platform provides "safe, transparent, fair, and affordable financial services."[4]

17. Uphold provides financial services and consumer accounts, including products to transfer currency and other consumer assets electronically. Uphold also offers various "wallets" that can "be used to make payments to vendors, send money to friends, and instantly convert your cryptocurrencies for other assets. It's a safe and secure way to use and transfer funds."[5]

A. Uphold Holds Itself Out as an Industry Leader in Account Security

18. Uphold recognizes the importance of maintaining the security of its customers' accounts and promises its millions of users that it will safeguard their accounts and their money from unauthorized access and security threats.

19. Uphold touts itself as a secure cryptocurrency platform and states on its website: "Security is in our DNA. Our number one priority is to protect you, your money, and your information. Security is built into our systems and culture."[6]

---

[3] *See* BusinessWire, *Earn up to 10% Interest on USD and Euro on Uphold* (June 3, 2019), https://www.businesswire.com/news/home/20190603005557/en/.
[4] *See* Uphold, Resources, available at https://uphold.com/en-us/resources/about (last visited April 18, 2022).
[5] *See* Uphold, Bitcoin Wallet, available at https://uphold.com/en-us/digital-wallet/bitcoin-wallet (last visited April 18, 2022).
[6] *See* Uphold, Security, available at https://uphold.com/en-us/get-started/security (last visited April 18, 2022).

20. Uphold purports to utilize multiple tools to secure its customers' accounts and makes the following representations:

- "[O]ur Information Security and Personal Information protection programs . . . are designed to meet or exceed regulatory requirements, establish the highest levels of trust with our members, and prevent bad actors from taking advantage of our systems, members, employees, or brand."[7]
- "We deploy layered defenses to limit the scope and depth of potential attacks, as well as sophisticated encryption."[8]
- "Security professionals routinely conduct security audits and penetration testing of our systems."[9]
- Bug Bounty Program - to encourage reporting of security vulnerabilities on the platform.[10]
- "The Uphold Security Operations Centre "monitors systems year-round and ***responds immediately*** to any detected threat."[11]
- "All our providers undergo appropriate due diligence checks. Special attention is paid to integrations incorporating sensitive data."[12]
- "The Uphold team are background checked by an accredited vendor. Mandatory security and privacy training is conducted regularly."[13]
- "We'll [ ] do email verification if we detect anything untoward. If we detect unusual activity, we'll send you an email to verify it is you."[14]
- "Uphold is a pioneer in our space when it comes to the security of our consumers: we are one of the first companies working with digital currencies to become certified to PCI/DSS [the Payment Card Industry Security Standards Council], one of the most stringent security standards in the industry. Being compliant means that we are doing our very best to

[7] *See* Uphold, Security at Uphold, available at https://support.uphold.com/hc/en-us/articles/203399367-Security-at-Uphold (last visited April 18, 2022).
[8] *See* Uphold, Security, available at https://uphold.com/en-us/get-started/security (last visited April 18, 2022).
[9] *Id.*
[10] *Id.*
[11] *Id.* (emphasis added).
[12] *Id.*
[13] *Id.*
[14] *Id.*

> keep our members' valuable information secure and out of the hands of people who could use that data in a fraudulent way."[15]

21. In or around July 2021, Mr. Yuille began looking for a secure cryptocurrency exchange to transfer Bitcoin. Mr. Yuille reviewed several different cryptocurrency platforms and ultimately chose to have his BTC transferred to Uphold because of its representations of account security, superlative customer service, Uphold's purported secure multifactor authentication, and the fact that Uphold claimed to monitor its platform for security threats 24 hours a day and every day of the year.

22. On August 23, 2021, pursuant to Uphold's inquiry, Mr. Yuille informed Uphold in writing that he was retired and the purpose of the account was:

a. to hold BTC;

b. to sell and reduce to dollars and transfer dollars to his bank; and

c. to trade crypto coins like those listed on Uphold.

23. Mr. Yuille trusted and relied on Uphold's representations that his assets would be safe with Uphold.

24. In August 2021, Mr. Yuille had approximately 106 BTC deposited in his account.

25. Despite the foregoing representations, Uphold breached its representations and duties to Mr. Yuille by, *inter alia*, failing to safeguard Mr. Yuille's data, information, and assets, and by allowing unauthorized third parties to gain access to Mr. Yuille's cryptocurrency account resulting in significant financial harm to Mr. Yuille, and Uphold further failed to comply with the EFTA.

[15] *Id.*

B. Uphold Was Aware of the Risk of Cyber-Attacks and Its Deficient Customer Support Services

26. Uphold was aware of the risk of cyber-attacks, account hacking, and potential improper transfers out of consumers' accounts, as evidenced from Uphold's own website, which features multiple articles addressing account security concerns and procedures.

27. Unfortunately, as Mr. Yuille learned, Uphold did not adhere to its own procedures and failed to restrict access to Mr. Yuille's account after he informed Uphold that his account may have been compromised.

28. Uphold has recognized the inadequacy of its customer support services. In the Uphold Help Center on Uphold's website, Uphold acknowledged that: "We haven't been able to provide anything like the customer service we'd like during this avalanche and recognize that we've let many of you down. We're deeply sorry. We appreciate that there's nothing more annoying than temporary account restrictions and slow response times."[16]

29. In that same post, Uphold also recognized a massive increase in activity by "scammers and bad actors," noting that their fraud and compliance policies and systems "are constantly contending with the advancements of scammers and bad actors, but were not optimized to cope with the 50x increase in volumes we've seen."[17]

30. In response to these inadequacies, Uphold imposed changes purportedly to improve customer support response time. For example:

- "We're slashing the number of situations in which we restrict your account - in fact, we're cutting it by almost half - as we reward lower-risk customers for good standing."[18]

[16] *See* Uphold, Improving our customer support, available at https://support.uphold.com/hc/en-us/articles/360057035232-Improving-our-customer-support (last visited April 18, 2022).
[17] *Id.*
[18] *Id.*

- "You'll have to contact customer service less because you'll be able to self-serve in the app for things like changing your email address or 2-factor authentication, without needing any help from us."[19]

- "We're introducing rules that mean if you make a mistake in your declared info - such as a digit wrong in your date of birth - you can correct it without having your account restricted."[20]

31. Many of these measures, while presumably meant to increase efficiency, weaken account security. These changes introduced security risk by reducing the number of situations when an account would be frozen based on suspicious activity, allowing users to "correct" key information without causing their account to be restricted, and allowing users (and unauthorized third parties) to change account email addresses and two-factor authentication more easily without going through customer service.

32. In short, Uphold knew of the risks that its customers' accounts could be comprised or hacked, knew that its own monitoring systems and procedures were inadequate to address those risks, and knew that it had an obligation to protect consumers from those risks. Yet it failed to take appropriate action to safeguard customers' data and information from being accessed by unauthorized third parties. Rather, Uphold altered its security policies and procedures to make it even *easier* for unauthorized third parties to gain access to Uphold's customers' accounts.

33. In addition, it appears that Uphold may have permitted Mr. Yuille's two-factor authentication to be turned off, modified, or accessed without Mr. Yuille's consent.

C. Uphold Did Not Comply with the EFTA

34. Adding insult to injury, when Uphold learns of a potentially compromised user account or unauthorized transfers, it places the account "under review." This review can take

[19] *Id.*
[20] *Id.*

months, if not longer, and almost invariably results in Uphold blaming the user rather than acknowledging the failures of its own system. Uphold's slow-moving investigation process, its failure to provide the EFTA-mandated disclosures to Mr. Yuille, and its failure to properly credit such unauthorized transfers violates the provisions of the EFTA and its implementing regulations.

35. The EFTA and its corresponding regulations implemented by the Consumer Financial Protection Bureau ("CFPB"), 12 C.F.R. § 1005.1, *et seq*. were designed with the "primary objective" of "the protection of individual consumer rights."[21]

36. The EFTA and its implementing regulations ("Regulation E") sets forth the following relevant definitions:

a. "[F]inancial institution" includes bank and credit unions, as well as "any other person who, directly or indirectly, holds an account belonging to a consumer." A "person" includes "a natural person or an organization, including a corporation[.]" 12 CFR § 1005.2G.

b. The term "account" means a consumer account established primarily for personal, family, or household purposes, but such term does not include an account held by a financial institution pursuant to a bona fide trust agreement.

c. A "consumer" is defined as a "natural person." 15 U.S.C. § 1693a(6).

d. An "error" includes, *inter alia*, an "unauthorized electronic fund transfer." 15 §1693f(f)(l); 12 C.F.R. § 1005.1 l(a)(vii).

e. An "unauthorized electronic fund transfer" is defined as "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit." 15 U.S.C. § 1693(a)(12); *see also* 15 C.F.R. § 1005(m). The CFBP (and the Board of Governors of the Federal Reserve System before it) have specifically stated that "[a]n unauthorized [electronic funds transfer] includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery."

[21] 15 U.S.C. § 1693; 12 C.F.R. §1005.l(b) (The "primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers and remittance transfers.").

37. A consumer has no liability for unauthorized EFTs if the financial institution has not provided required disclosures. 12 CFR § 1005.6(a).

38. If the required disclosures have been made, Regulation E limits a consumer's responsibility for an unauthorized EFT. For unauthorized EFTs resulting from the "loss or theft of an access device," consumer liability is capped at a maximum of $50, provided the consumer notifies its financial institution within two (2) business days of learning of the loss or theft of an access device, or $500 if the consumer gives notice after two (2) days but within sixty (60) days. 12 CFR § 1005.6(b)(1)-(2).[22]

39. Financial institutions like Uphold must provide initial disclosures of the terms and conditions of EFT services before the first EFT is made or at the time the consumer contracts for an EFT service. Uphold is obligated to give a summary of various consumer rights under the regulation, including the consumer's liability for unauthorized EFTs, the types of EFTs the consumer may make, limits on the frequency or dollar amount, fees charged by the financial institution, and the error-resolution procedures.

40. The EFTA and Regulation E require that after a financial institution receives oral or written notice of an error—which is defined to include an unauthorized EFT—from a consumer, the financial institution must do all of the following:

a. Promptly investigate the oral or written allegation of error;

b. Complete its investigation within ten (10) business days;

c. Report the results of its investigation within three (3) business days after completing its investigation; and

[22] An "access device" means "a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers." 12 CFR § 1005.2(a)(1).

d. Correct the error within one (1) business day after determining that an error has occurred.[23]

41. If the financial institution determines that an error occurred, it has the option to either (1) timely correct the error, including the crediting of interest where applicable; or (2) timely provisionally recredit the consumer's account for the amount alleged to be in error pending the conclusion of the institution's investigation of the error within ten (10) business days of being notified of the error. 15 U.S.C. § 1693f(c); *see also* 12 C.F.R. § 1005.11. In no circumstance can an investigation be concluded more than forty-five (45) days after receipt of the notice of error, and during the pendency of the investigation, the consumer must be allowed full use of funds provisionally recredited.

42. Where a financial institution (1) fails to provisionally recredit a consumer's account within the ten-day period specified above, and the financial institution (a) did not make a good faith investigation of the alleged error, or (b) did not have a reasonable basis for believing that the consumer's account was not in error, then the consumer shall be entitled to treble damages determined under section 1693m(a)(1).

43. Uphold failed to comply with the aforementioned provisions.

44. Under the EFTA, Uphold is a financial institution; Mr. Yuille is a consumer; Mr. Yuille's accounts were accounts established for personal, family, or household purposes; and the transactions at issue were EFTs and were unauthorized.

D. Uphold Breached Its Legal Duties to Mr. Yuille, Exposing Mr. Yuille to the Loss of Approximately $5,000,000 of Mr. Yuille's Assets

45. Uphold's failure to implement adequate security measures and failure to protect Mr. Yuille's account from unauthorized access—both before and after Mr. Yuille notified Uphold

[23] 12 CFR § 1005.11(c)(1).

that his account had been compromised—led to the swift and unauthorized transfer of nearly $5,000,000 of cryptocurrency assets out of Mr. Yuille's cryptocurrency account.

46. Between December 7 and 9, 2021, an unauthorized third party attempted to change the password associated with Mr. Yuille's Uphold account and failed on five (5) separate occasions.

47. On December 7, 2021, at 8:01 p.m., a third party unsuccessfully attempted to log in to Mr. Yuille's account *from Nigeria*.

48. Then, on December 9, 2021, at 10:48 a.m., an unauthorized party changed Mr. Yuille's Uphold password. Eight minutes later, that individual successfully changed the e-mail associated with Mr. Yuille's account.

49. The foregoing was performed without Mr. Yuille's permission or knowledge.

50. Later that day, Mr. Yuille attempted to log in to his Uphold account on at least three separate occasions, but was unable to do so because the e-mail address and password associated with his Uphold account had been changed without his knowledge.

51. Following his unsuccessful login attempts, Mr. Yuille sent the following panicked message to Uphold on December 9, 2021, at 4:41 p.m.:

bruce howard yuille December 9, 2021 at 4:41 PM

This is a follow-up to your previous request #1536190 "I request an increase cash ..."

Uphold Support:

HELP, I am locked out of my account. I enter the username and password I have been using for past several months, and I get a message that they do not match your records. I try to reset password, and although you send message saying you will send me instructions, nothing is sent. I have repeated the above at least 3 times.

I placed a limit order to sell .5 bitcoins, and you send me notice ON DEC.7 that it was executed. I used the same username and password today that I used to place that order. WHAT IS GOING ON?

Please communicate with me.

Bruce Yuille

52. Even though Mr. Yuille informed Uphold that he had been using the same username and password for "several months" and Uphold knew that both the e-mail address and password for Mr. Yuille's Uphold account had been modified just six (6) hours earlier, Uphold's customer service representative responded only by telling Mr. Yuille to check his spam for the verification e-mail(s). This is especially surprising in light of the numerous, recent failed attempts to change Mr. Yuille's Uphold password, a failed attempt emanating from Nigeria to access Mr. Yuille's Uphold account, and the ultimate change of the e-mail address and password for Mr. Yuille's Uphold account.

53. Had Uphold conducted any reasonable diligence associated with the foregoing, it would have realized that Mr. Yuille's account had been hacked and then would have frozen the account, thereby preventing the unauthorized transfer of assets out of Mr. Yuille's account. But instead of taking appropriate steps to safeguard Mr. Yuille's assets, Uphold did nothing.

54. Beginning approximately eight (8) hours after Mr. Yuille's panicked e-mail and continuing through around 5:00 p.m. on December 11, 2021, Uphold permitted approximately $5,000,000 worth of BTC to be transferred out of Mr. Yuille's Uphold account. And Uphold permitted those transfers notwithstanding myriad suspicious and alarming activity and Mr. Yuille himself alerting Uphold to significant issues associated with his account access.

55. Uphold had notice of the security concerns regarding Mr. Yuille's account as early as December 9, 2021. Despite Uphold's many assurances on its website that account security is the company's priority and its representation that it "monitors systems year-round and responds immediately to any detected threat," Uphold failed to take any action in response to the open and obvious threat to Mr. Yuille's account. Uphold's representations regarding the security and safety of its platform were false.

56. Had Uphold timely locked, restricted access, or restricted transfers out of Mr. Yuille's account, the unauthorized third party would not have been able to transfer any assets out of Mr. Yuille's Uphold account.

57. Uphold has a duty to protect its customers' assets and to promptly protect accounts. Uphold is aware of the grave threat posed by unauthorized access to customer accounts and must take appropriate steps to safeguard customer assets. Uphold failed to discharge its duties to Mr. Yuille and permitted approximately $5,000,000 worth of BTC to be electronically transferred out of Mr. Yuille's account over a two-day period—all without Mr. Yuille's authorization and all made possible through Uphold's misrepresentations, gross negligence, statutory violations, and other wrongdoing.

58. Uphold failed to provide reasonable and appropriate security to prevent unauthorized access to its customer's account and wallet, and the assets stored therein.

59. Among other things, Uphold:

a. misrepresented the safety and security of funds entrusted to it;

b. failed to adequately safeguard and protect its customer's account and the consumer assets stored therein;

c. failed to use readily available security measures to prevent or limit unauthorized access to customer accounts and to prevent unauthorized transactions from occurring on those accounts;

d. failed to suspend user credentials after a certain number of unsuccessful access attempts;

e. lacked proper monitoring solutions and failed to monitor its systems for the presence of unauthorized access in a manner that would enable Uphold to detect the intrusion and take steps to restrict such unauthorized access;

f. failed to implement defenses to identify unauthorized third parties such as delaying transfers from accounts on which the password was recently changed or simply delaying transfers from accounts to allow for additional verifications from customers; and

g. failed to implement reasonable means for customers to contact Uphold without undue delay after discovering account security issues;

h. failed to implement policies and procedures to promptly act after being notified by a customer that they cannot access their account or suspect an account has been compromised, including by timely locking the account, restricting access to the account, or restricting transfers from the account until the account is secured; and

i. failed to act reasonably and adequately—by timely locking the account, restricting access to the account, or restricting transfers from the account until the account was secured—after being notified that a customer could not access their account or suspected their account had been compromised.

60. Uphold's security measures were inadequate to protect its customers, including Mr. Yuille. As a result of inadequate security practices and procedures, Uphold created an unreasonable risk of unauthorized access to customer accounts, including that of Mr. Yuille, and unauthorized transfer of assets out of customer accounts, including Mr. Yuille's.

61. The cryptocurrency transfers out of Mr. Yuille's accounts would not have occurred but for Uphold's failure to maintain proper security measures to prevent unauthorized access to Mr. Yuille's account and Uphold's failure to adequately protect Mr. Yuille's account and associated personal data.

62. The unauthorized transfers from Mr. Yuille's account were electronic funds transfers under the EFTA, 15 U.S.C. §§ 1693, *et seq.*

63. Mr. Yuille gave notice that he was locked out of his account on December 9, 2021. After having notice that Mr. Yuille's account had been compromised, however, Uphold failed to take any action whatsoever (such as, for example, freezing the account) but, rather, allowed the rest of the unauthorized transfers to occur.

64. Additionally, Uphold failed to investigate the unauthorized transfers and inform Mr. Yuille of the result of such investigation within the time periods required by the EFTA.

65. Because the transfers from Mr. Yuille's account were unauthorized, Uphold was obligated to credit the unauthorized transfers back to Mr. Yuille's account as required by the EFTA. To date, however, Uphold has not credited any of the unauthorized transfers back to Mr. Yuille's account.

66. In refusing to credit Mr. Yuille's account, Uphold did not have a good-faith basis to conclude that Mr. Yuille's account was not in error and, on information and belief, willfully and knowingly concluded that Mr. Yuille's account was not in error when it did not have evidence to reach such a conclusion.

CLAIMS ASSERTED

COUNT I
VIOLATION OF EFTA AND REGULATION E CUSTOMER SERVICE PROVISIONS
15 U.S.C. § 1693; 12 C.F.R. § 1005.11(a)(7); 12 C.F.R. § 1005.7

67. Mr. Yuille incorporates by reference the allegations in the paragraphs 1 through 66.

68. The EFTA, 15 U.S.C. § 1693f(f)(6) and Regulation E, 12 C.F.R. § 1005.11(a)(7), (c) require financial institutions to address "a consumer's request for additional information or clarification concerning an electronic fund transfer" within ten business days of receiving notice of error, or within 45 calendar days if the financial institution provisionally recredits the consumer's account, with interest where applicable, within 10 business days of receiving the notice of error.

69. As alleged above, Mr. Yuille is a "consumer" within the meaning of the EFTA and Regulation E.

70. Uphold, a "financial institution" as alleged herein, has violated the EFTA and Regulation E by failing to timely provide information or clarification concerning electronic fund

transfers, including requests by Mr. Yuille made to determine whether there were unauthorized electronic transfers from his account. *See* 15 U.S.C. § 1693f(f)(6); 12 C.F.R. §1005.11.

71. Mr. Yuille has been damaged directly by Uphold's acts, errors, and omissions in an amount that will be proven at trial.[24] Because Uphold's misconduct directly caused Mr. Yuille's damages, Uphold must be found liable for Mr. Yuille's damages.

72. To enforce his rights, Mr. Yuille has retained undersigned counsel and is obligated to pay counsel a reasonable fee for its services.

73. Mr. Yuille is entitled to compensatory damages, attorneys' fees, and costs under 15 U.S.C. § 1693m, as well as treble damages under 15 U.S.C. § 1693f(e), on this claim.

COUNT II
VIOLATION OF N.Y. BUS. LAW § 349

74. Mr. Yuille incorporates by reference the allegations in paragraphs 1 through 66.

75. As alleged above, Uphold is a cryptocurrency exchange and digital money platform based in the State of New York with more than 1.7 million customers globally and nearly $6 billion in transactions since its inception. Uphold describes itself as a "multi-asset digital money platform offering financial services to a global market."

76. Uphold's wrongdoing took place in New York, where Uphold's principal place of business is.

77. Uphold engages in consumer-oriented conduct when it holds itself out as being one of the most secure cryptocurrency platforms and touts as such on its website.

[24] Uphold's limitation of liability and purported disclaimer set forth in Uphold's General Terms and Conditions, last updated January 28, 2020 (the "Terms and Conditions") are not enforceable against Mr. Yuille because they are unconscionable, void as against public policy, and attempt to disclaim clear, non-waivable legal obligations.

78. Uphold engaged in consumer-oriented conduct with respect to Mr. Yuille on a similar basis with other potential customers in promoting its secure cryptocurrency to attract customers like Mr. Yuille.

79. Uphold used a deceptive or unfair act or practice by: (1) misrepresenting the safety and security of the assets entrusted to it; (2) failing to disclose to Mr. Yuille that Uphold's platform was not secure and sufficient to safeguard his assets; (3) failing to properly monitor activity on its platform; and (4) deliberately or recklessly failing to safeguard and protect Mr. Yuille's personal information and assets contained in Mr. Yuille's account after enticing Mr. Yuille to place significant assets in his Uphold account through promotion of Uphold's purportedly secure platforms.

80. Mr. Yuille has been damaged directly by Uphold's acts, errors, and omissions in an amount that will be proven at trial. Because Uphold's misconduct directly caused Mr. Yuille's damages, Uphold must be found liable for Mr. Yuille's damages.

81. Mr. Yuille is entitled to compensatory damages, attorneys' fees, and costs as well as treble damages under N.Y. Bus. Law § 349(h) on this claim.

COUNT III
VIOLATION OF THE MICHIGAN CONSUMER PROTECTION ACT, MCLS § 445.901, *et. seq.*

82. Mr. Yuille incorporates by reference the allegations in paragraphs 1 through 66.

83. Uphold's offering of financial services as a cryptocurrency exchange constitutes "trade or commerce" within the meaning of § 445.902(1)(g) of the Michigan Consumer Protection Act ("MCPA").

84. Uphold failed to safeguard and protect Mr. Yuille's personal information and assets contained in Mr. Yuille's account after enticing Mr. Yuille to place significant assets in his Uphold account through promotion of Uphold's purportedly secure platforms.

85. Per § 445.903(e) of the MCPA, Uphold represented that its services in providing a secure platform for cryptocurrency exchange were of a particular standard or quality when in fact they were not of that standard or quality because Uphold could not secure its customers' personal information or assets.

86. Mr. Yuille is entitled to compensatory damages, attorneys' fees, and costs under § 445.911(2) of the MCPA on this claim.

COUNT IV
INTENTIONAL MISREPRESENTATION

87. Mr. Yuille incorporates by reference the allegations in paragraphs 1 through 66.

88. Uphold made misrepresentations of presently existing fact when it held itself out as being one of the most secure cryptocurrency platforms and touts as such on its website.

89. Uphold made further misrepresentations on its website when it made the following statements:

- "We deploy layered defenses to limit the scope and depth of potential attacks, as well as sophisticated encryption."[25]
- "Security professionals routinely conduct security audits and penetration testing of our systems."[26]
- "The Uphold Security Operations Centre "monitors systems year-round and ***responds immediately*** to any detected threat."[27]

[25] *See* Uphold, Security, available at https://uphold.com/en-us/get-started/security (last visited April 18, 2022).
[26] *Id.*
[27] *Id.* (emphasis added).

- "We'll [ ] do email verification if we detect anything untoward. If we detect unusual activity, we'll send you an email to verify it is you."[28]

90. Uphold intended for potential customers like Mr. Yuille to rely on these misrepresentations.

91. Mr. Yuille relied on these misrepresentations and placed significant assets in his Uphold account.

92. Mr. Yuille would not have placed significant assets in his Uphold account but for Uphold's misrepresentations that it was a secure cryptocurrency platform and that the Uphold Security Operations Centre immediately responds to any detected threat.

93. Mr. Yuille has been damaged directly by Uphold's acts, errors, and omissions in an amount that will be proven at trial. Because Uphold's misconduct directly caused Mr. Yuille's damages, Uphold must be found liable for Mr. Yuille's damages.

94. Mr. Yuille is entitled to compensatory damages, attorneys' fees, and costs.

COUNT V
NEGLIGENCE

95. Mr. Yuille incorporates by reference the allegations in paragraphs 1 through 66.

96. Uphold owed Mr. Yuille a duty to act reasonably and with due care and not to act negligently or grossly negligently.

97. Uphold had a duty to exercise reasonable care in safeguarding and protecting Mr. Yuille's personal information and assets contained in Mr. Yuille's account.

98. Uphold had a duty to keep such data from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

[28] *Id.*

99. Uphold had a duty to comply with its own policies, procedures, and legal duties and to maintain the security of Mr. Yuille's personal account.

100. Uphold had a duty to implement reasonable security measures to prevent unauthorized transactions from occurring on Mr. Yuille's account and wallet.

101. Uphold had a duty to implement reasonable procedures to detect security breaches and timely act to secure such breaches.

102. Uphold breached these duties by failing to safeguard and protect Mr. Yuille's account, including the associated personal information and consumer assets stored on Uphold's platform.

103. Uphold breached these duties by failing to adopt, implement, and maintain proper security measures to ensure that Mr. Yuille's account was adequately secured and protected and to prevent unauthorized access to his account.

104. Uphold breached these duties by failing to comply with industry standards and establish reasonable measures to protect Mr. Yuille's account and the assets stored on Uphold's platform.

105. Uphold breached these duties by failing to take reasonable and adequate steps to secure and protect Mr. Yuille's account after it knew or should have known that Mr. Yuille's account was compromised.

106. The breaches of these duties caused Mr. Yuille's loss of cryptocurrency in his Uphold account.

107. Mr. Yuille is entitled to compensatory and punitive damages on this claim.

COUNT VI
GROSS NEGLIGENCE

108. Mr. Yuille incorporates by reference the allegations in paragraphs 1 through 66.

109. Uphold owed Mr. Yuille a duty to act reasonably and with due care and not to act negligently or grossly negligently.

110. Uphold had a duty to exercise reasonable care in safeguarding and protecting Mr. Yuille's personal information and assets contained in Mr. Yuille's account.

111. Uphold failed even to exercise slight care in safeguarding Mr. Yuille's account.

112. Uphold demonstrated a reckless disregard for Mr. Yuille's rights when, after having notice that Mr. Yuille's account had been compromised, Uphold failed to take any action whatsoever (such as, for example, freezing the account) but, rather, allowed the unauthorized transfer of assets out of Mr. Yuille's Uphold account.

113. The breaches of these duties caused Mr. Yuille's loss of cryptocurrency in his Uphold account.

114. Mr. Yuille is entitled to compensatory and punitive damages on this claim.

COUNT VII
DECLARATORY JUDGMENT 28 U.S.C. § 2201

115. Mr. Yuille incorporates by reference the allegations in paragraphs 1 through 66.

116. Section 12.4 of Uphold's Terms and Conditions seeks to limit Uphold's liability to the actual fees paid by a customer such as Mr. Yuille in the preceding three months or $100.

117. Section 12.4 of Uphold's Terms and Conditions further seeks to disclaim any liability for any lost profits or other consequential, special, indirect or incidental damages arising out of or in connection with the Terms and Conditions.

118. Uphold's purported disclaimer and limitation of liability and indemnification is unenforceable because it is unconscionable, void as against public policy, attempts to disclaim statutory and other legal duties for which it cannot avoid contractually, and violates 15 U.S.C. §

1693l, which provides that a consumer may not waive by agreement any right conferred, or cause of action created, by the EFTA.

119. Mr. Yuille is entitled to a declaration that Uphold's purported disclaimer and limitation of liability in Section 12.4 of the Terms and Conditions is unenforceable.

WHEREFORE, Mr. Yuille prays for judgment against Uphold as follows:

a. damages based on fairness and equity;

b. compensatory damages currently estimated to be in excess of $5,000,000;

c. treble damages of approximately $15,000,000 pursuant to the EFTA and N.Y. Bus. Law §349;

d. reasonable attorneys' fees, costs, and expenses incurred pursuant to the EFTA, N.Y. Bus. Law § 349, and MCLS § 445.901;

e. prejudgment and post-judgment interest at the statutory rate;

f. a declaration that the Uphold's limitation of liability, disclaimer of liability, and related contractual language is unenforceable because it is unconscionable, void as against public policy, and violates the EFTA;

g. an award of any and all additional damages recoverable under law including but not limited to punitive damages, incidental damages, and consequential damages; and

h. such other and additional relief as the tribunal may deem just and proper.

DEMAND FOR JURY TRIAL

Mr. Yuille hereby demands trial by jury.

August 31, 2022

Respectfully submitted,

SPIRO HARRISON

By: /s/ Thomas M. Kenny
Jason C. Spiro
Thomas M. Kenny
363 Bloomfield Avenue, Suite 2C
Montclair, NJ 07042
Tel.: (973) 232-0881
tkenny@spiroharrison.com
jspiro@spiroharrison.com

Attorneys for Plaintiff

- and -

By: /s/ Brian Levin, Esq.
Brian Levin, Esq.
(*pro hac vice application forthcoming)*
LEVIN LAW, P.A.
2665 South Bayshore Drive, PH-2B
Miami, Florida 33133
Tel.: (305) 402-9050
brian@levinlawpa.com

By: /s/ Jeffrey B. Kaplan
Jeffrey B. Kaplan, Esq.
(*pro hac vice application forthcoming)*
DIMOND KAPLAN & ROTHSTEIN, P.A.
2665 South Bayshore Drive, PH-2B
Miami, Florida 33133
Tel: (305) 374-1920
jkaplan@dkrpa.com